UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Blue/Black Samsung Galaxy Note 9 Cell Phone SM N960U, Black LG Cell Phone marked for use with Verizon, Black Samsung Galaxy Cell Phone, Silver Lenovo Yoga Laptop Computer that are all presently in the possession of the United States Secret Service, which is located at 2707 North 108th St., Omaha, NE 68164

Case No. 8:19MJ71

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of Nebraska, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Section 1029	Fraud and related activity in connection with access devices

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

USSS SA Justin R. Larson
Printed name and title

- ☑ Sworn to before me and signed in my presence.
- ☐ Sworn to before me by telephone or other reliable electronic means.

Date: 2-12-19

Judge's signature

City and state: Omaha, Nebraska

Susan M. Bazis, U.S. Magistrate Judge
Printed name and title

Affidavit of Justin R. Larson

I, Justin R. Larson, being first duly sworn depose and say:

Section 1- PROFESSIONAL IDENTITY AND EXPERIENCE

1. I am a Special Agent with the United States Secret Service, assigned to the Omaha, Nebraska Resident Office. I have been employed as an agent with the Secret Service since May 2007.
2. In my official capacities with the Secret Service, I have investigated numerous cases involving the manufacture and negotiation of counterfeit U.S. securities of the state and private entities, wire fraud, money laundering and other complex financial crimes investigations. In addition to my experience, I have attended various seminars and training classes, which include those taught by the Federal Law Enforcement Training Center and the United States Secret Service Academy.

Section 2 – REASON FOR AFFIDAVIT

3. Affiant submits this application and affidavit in support of a search warrant authorizing a search of the computer, electronic equipment, and storage devices obtained from ANTHONY JAMES HANEL and COURTNEY LAPARELE CLARK, specifically:
    a. Blue/Black Samsung Galaxy Note 9 Cell Phone SM N960U
    b. Black LG Cell Phone marked for use with Verizon
    c. Black Samsung Galaxy Cell Phone
    d. Silver Lenovo Yoga Laptop Computer

The items are further described in **Attachment A** to this Application. Located within the equipment and devices to be searched, Affiant seeks to seize evidence, fruits, and

instrumentalities of criminal violations, including Fraud and related activity in connection with access devices, in violation of Title 18, United States Code, § 1029. Affiant requests authority to search the computer, computer media, and cellular phones specified in **Attachment A**, attached to this Application, and to seize all items listed in **Attachment B** as instrumentalities, fruits, and evidence of crime.

Section 3 - DETAILS OF INVESTIGATION AND PROBABLE CAUSE

4. This case originated from a call to the Affiant from officers of the Omaha Police Department ("OPD"). Those officers advised that they had arrested ANTHONY J HANEL and COURTNEY L CLARK for the Nebraska state crimes of possession of a defaced firearm, possession of a controlled substance - heroin, unlawful transport of a firearm, possession of a financial transaction device four or more, possession of a blank financial transaction device two or more, and possession of a forgery machine. Additionally, CLARK was also booked for the crime of obstruction and HANEL was also booked for charges of criminal impersonation and two counts of possession of a firearm by a felon.

5. Omaha Police officers reported to the Affiant the following:

    a. ANTHONY J. HANEL and COURTNEY L. CLARK were pulled over by OPD for the traffic violation of failure to signal an intent to change lanes while driving a blue Dodge Durango. The traffic stop occurred in the area of the 42nd Street exit on eastbound Interstate 80 is in the District of Nebraska. CLARK was the driver of the vehicle. HANEL was the front seat passenger. Initially, HANEL provided a false name and produced fictitious identification documents in the name of Robert M. Ogborn (11/26/86, WA DL). Nebraska State Patrol had to be called to the scene and ran a portable AFIS check on HANEL to determine his true identity.

b. During the traffic stop, an OPD narcotics detecting K9 was called to the scene to conduct a free air sniff of the vehicle. The K9 is a certified police narcotics detector dog in the State of Nebraska. The K9 detected the odor of narcotics in the blue Dodge Durango. A probable cause search was conducted. During this search, officers located a pelican travel case in the third row of the Dodge Durango. Inside the pelican case, the officers located a credit card machine that is commonly used to add names to a card or to alter credit cards to match identification. Officers also found a large number of blank cards (commonly referred to as "white plastic"). Officers found 18 cards that were partially complete. Officers located 44 cards in the name of Robert Ogborn (this may actually be 47, since 3 were found in a wallet in the front of the vehicle and it is unclear if they are included or not) all with different card numbers. There were 7 cards in the name of Anthony James with different card numbers. There was 1 card in the name of Jonathan Fortner. There were 2 cards in the name of Anthony HANEL with different card numbers. In short, there were 53 (possibly 56) completed credit cards within the vehicle in 4 different peoples' names. There were also 44 gift cards located throughout the vehicle and each had a different value written on them.

c. Officers also found in the vehicle three cellular phones within the vehicle ("the cellular phones"). A blue/black Samsung Galaxy Note 9 Cell Phone SM N96OU (IMEI 358621092460188) was found within the vehicle during the initial search when the vehicle was located along Interstate 80. Two cellular phones were found during the course of an inventory search: a black LG Cell Phone marked with Verizon and a black Samsung Galaxy Cell Phone (IMEI 353756071856926).

Officers also found a silver Lenovo Yoga laptop computer (serial number PF0D3XYY) ("the laptop") in the vehicle during an inventory search.

d. Officers also found a small black pouch in the third row seat which contained a small amount of heroin that weighed approximately 1 gram and field tested positive as heroin. In the third row, officers also found a black Coach brand back pack. Inside the back pack were two handguns and two hand gun magazines. One of the handguns was a Sig Sauer 9mm with a defaced serial number. The other handgun had been painted so officers could not see the make of the handgun, but it appeared to be a .22 caliber 1911 model handgun with the serial number A365580.

e. Your Affiant has consulted with an Industry Operations Investigator from the Bureau of Alcohol, Tobacco, and Firearms and was advised that there are no Sig Sauer manufacturing facilities in Nebraska, meaning that the Sig Sauer firearm would have had to have been transported in interstate commerce to be found in the State of Nebraska.

f. Based on an NCIC query, I found that ANTHONY HANEL is a convicted felon with his most recent felony conviction being from March 23, 2017 for Possession of a Controlled Substance. HANEL has a prior history of forgery, identity theft, possession with intent to distribute-controlled substances, manufacturing of controlled substances, burglary, and firearms possession.

g. Based on an NCIC query, I found that COURTNEY CLARK is not a felon and has no active arrest warrants. Both HANEL and CLARK were transported to the Douglas County Corrections facility where they declined to speak with officers and requested an attorney. All of the items obtained from the search warrant, including

the cellular phones and the laptop, were transported to the Omaha Police Department and placed into evidence and are presently in the custody and possession of the United States Secret Service. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Secret Service.

6. Affiant has began investigation into the access cards that were recovered from Hanel and Clark's, and these devices show activity in such states as Washington, California, Utah, Wyoming, Colorado, and Nebraska dating to as early as January 11, 2019.

7. The statements in this affidavit are based in part on information provided by various police departments and witnesses, more specifically set forth in this Affidavit, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities constituting evidence of criminal violations of federal law are presently located within the electronic devices, specifically the cellular phones and the laptop, listed in **Attachment A**.

Section 4- DEFINITIONS:

8. The following definitions apply to this Affidavit and Search Warrant:

"**Computer**," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device";

"**Computer hardware**," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks);

"**Computer software**," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities;

"**Computer-related documentation**," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items;

"**Computer passwords and data security devices**," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include

programming code that creates "test" keys or "hot" keys, which preform certain preset security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it;

"**Records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

"Electronic Media Storage" as used herein means any device designed to or capable of storing data or holding data in electronic format. (i.e. Hard Drive, Thumb Drives, Flash Memory, Floppy Disks, Compact Discs, DVDs.

A **"wireless telephone" (or mobile telephone, or cellular telephone)** is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A

wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet.

Section 5: SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS:

9. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

10. There is probable cause to believe that things that were once stored on the cellular phones and the laptop may still be stored there, for at least the following reasons:

    a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

11. Based on your affiant's knowledge, training, and experience, and the experience of other law enforcement personnel, your affiant knows that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting such as an office or

laboratory. The analysis of computer and/or digital media is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover digital information, to include hidden, erased, compressed, password-protected or encrypted files. The high volume of the contents and the potential intentional concealment of criminal activity through random ordering and deceptive file names may require the examination of all stored data. This process may take weeks or months depending on the volume of the data involved and the caseload of the computer expert. One such forensic and controlled laboratory environment is at the United States Secret Service Kansas City Field Office (KCM), which is physically located in Kansas City, Missouri.

12. Recognizing that specialized and highly technical equipment and software will be needed to conduct the analysis of the previously seized digital media, the media will likely be examined in the KCM lab or by another trained forensic examiner within the state of Nebraska. Additionally, under limited situations, assistance may be required by the receiving laboratory from other qualified laboratories. I know that a specialized examiner is required because of the following:

    a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives, CDs, DVDs, PDAs, MMCs, memory sticks and optical disks) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files is evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the

volume of data stored, and it would be impractical to attempt this kind of data search on site;

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification of destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

c. The size of electronic storage media continues to grow, creating a large amount of data that must be searched to locate specific items. To place this in perspective, 250 GB hard drive can contain:

   i. up to 93,750 digital images;

   ii. up to 221 days of around-the-clock MP3 ;

   iii. up to 375 hours of VHS quality video or; 106 two-hour DVD-quality video.

13. Based on your affiant's consultation with experts in computer searches, data retrieval from computers and related media and from his consultations with other law enforcement officers who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of the computers system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

    a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system (known as dongles). It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the input/output devices, software, documentation, data security devices are not necessary to

retrieve and preserve the data after inspection, the government will return them in a reasonable period of time;

14. In order to fully retrieve data from a computer system, the analyst also needs all electronic storage devices. Further, the analyst again needs all the system software (operating systems or interfaces and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval; and

15. As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cellular phones and the laptop were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the cellular phones and the laptop because:

    a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

    b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

    c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper

context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

16. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the cellular phones and the laptop consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

17. *Manner of execution*. Because this warrant seeks only permission to examine the cellular phones and the laptop which are already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I

submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Section 6- SUMMARY:

18. Based on the foregoing, there is probable cause to believe that violations of federal law, including but not limited to, Title 18 U.S.C. § 1029 have been committed, and that the property, evidence, fruits and instrumentalities of these offenses, more fully described in **Attachment B** of this Application, are located in the electronic devices more specifically described in **Attachment A** to this Application. I respectfully request that this Court issue a search warrant for the electronic items, authorizing the search of the items described in **Attachment A** of this Application.

FURTHER AFFIANT SAYETH NOT,

Justin R. Larson
Special Agent
United States Secret Service

Subscribed and sworn to before me this 12 day of February, 2019.

SUSAN M. BAZIS
United States Magistrate Judge

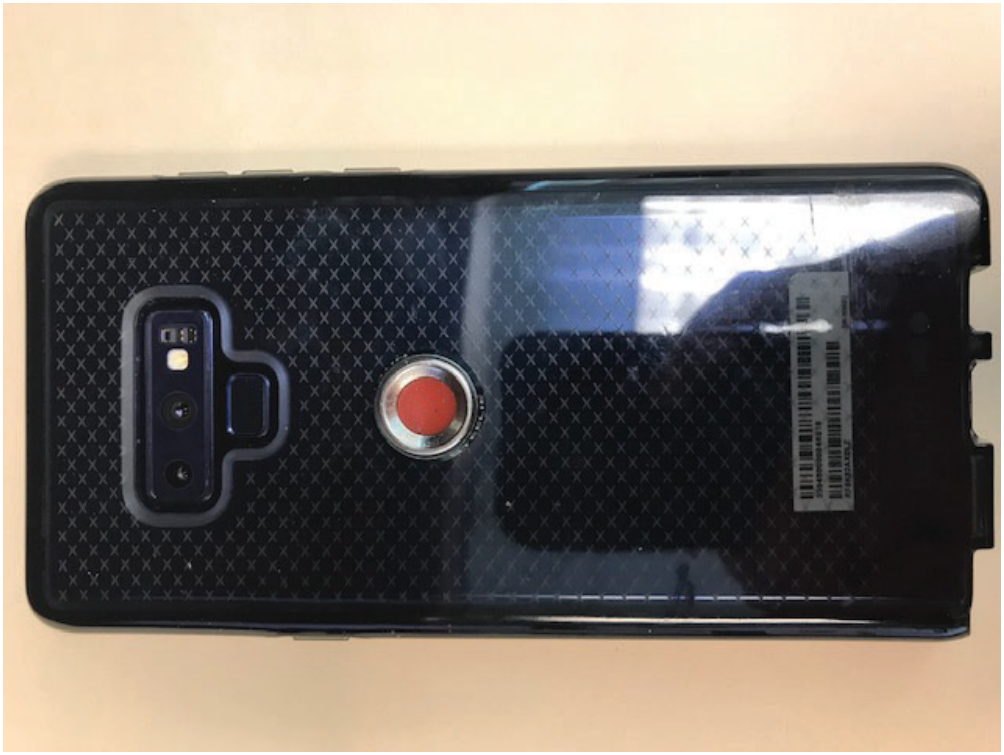
ATTACHMENT A

ITEMS TO BE SEARCHED

This warrant applies to the following items that are all presently in the possession of the United States Secret Service, which is located at 2707 North 108th St., Omaha, NE 68164:

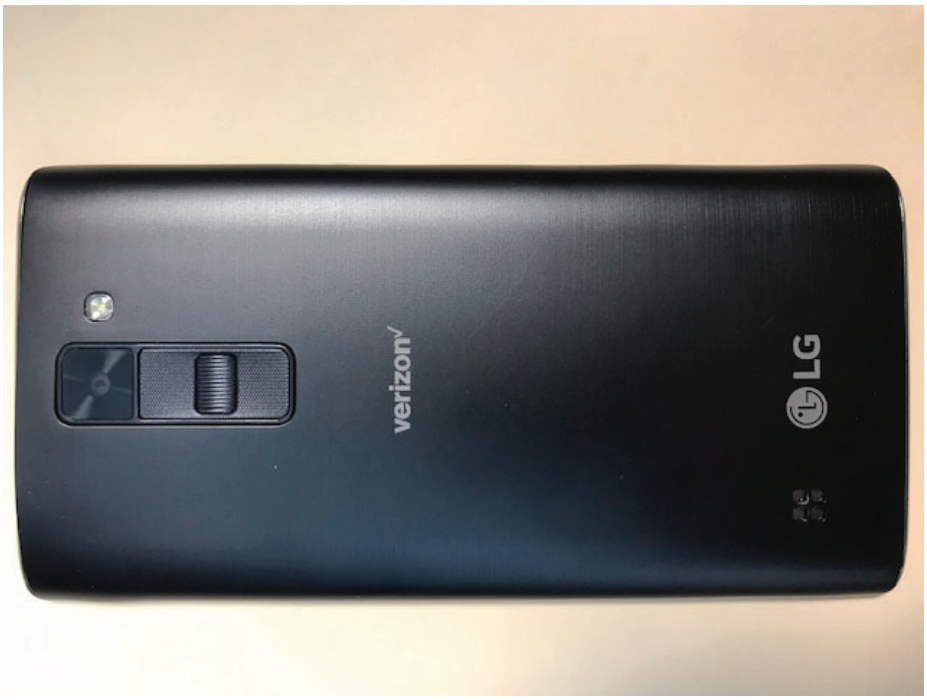
Item #1

Blue/Black Samsung Galaxy Note 9 Cell Phone SM N96OU, IMEI 358621092460188 originally discovered in the suspects' rental vehicle when parked on I-80 East at South 42nd St., Omaha, NE. This item was booked into the computer evidence system of the Omaha Police Department as item #8 under case number AL30847.



Item #2

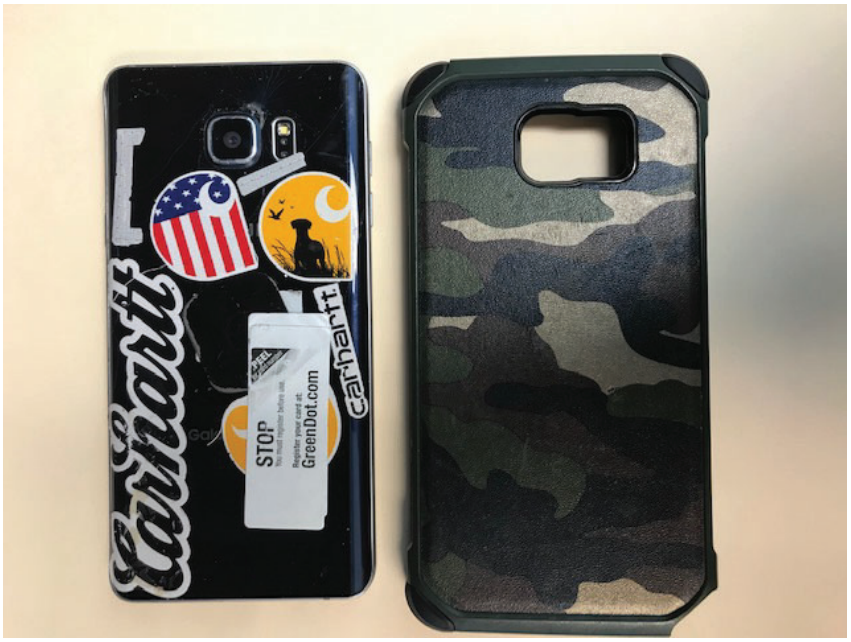
Black LG Cell Phone marked for use with Verizon originally discovered in the suspects' rental vehicle when inventoried at 7809 F St., Omaha, NE 68127. This item was booked into the computer evidence system of the Omaha Police Department as item #15 under case number AL30847.



Item #3

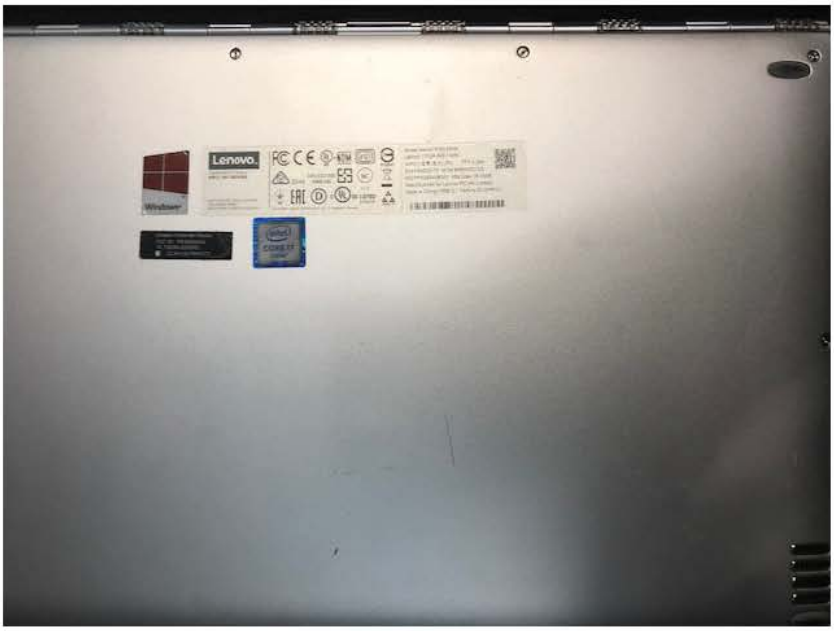
Black Samsung Galaxy Cell Phone IMEI 353756071856926 originally discovered in the suspects' rental vehicle when inventoried at 7809 F St., Omaha, NE 68127. This item was booked into the computer evidence system of the Omaha Police Department as item #16 under

case number AL30847.



Item #4

Silver Lenovo Yoga laptop Computer Serial number PF0D3XYY discovered in the suspects' rental vehicle when inventoried at 7809 F St., Omaha, NE 68127. This item was booked into the computer evidence system of the Omaha Police Department as item #17 under case number AL30847.


Lenovo

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED

The following items, which may be evidence, fruits, and instrumentalities of violations of Fraud in connection with Fraud and Related Activity in Connection with Access Devices (18 U.S.C. § 1029) are to be searched for and/or seized:

1. Any computers or electronic media, including computer hardware, electronic or magnetic storage devices, such as floppy diskettes, hard disks, backup tapes, CD-ROMs, CD-Rs, CD-RWs, DVD-ROMs, DVD-Rs, DVD+Rs, DVD-RWs, DVD+RWs, optical discs, printer buffers, smart cards, USB thumb drives, USB drives, USB Flash Memory, Firewire Devices, Smart Media, Memory Sticks, Multimedia Cards (MMC), Secure Digital Cards, memory calculators, electronic dialers, Bernoulli drives, electronic notebooks, personal digital assistants, and any data, image or information that is capable of being read or interpreted by computer; that were or may have been used as a means to commit the offenses described in the affidavit.
2. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

3. All records, documents and materials related to ANTHONY JAMES HANEL and COURTNEY LAPARELE CLARK;

4. All records, documents, and materials related to the fraudulent use or creation of access devices;

5. Hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, printouts of computer photographs, graphic interchange formats and/or photographs, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG); notations of any passwords that may control access to a computer operating system or individual computer files;

6. Any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation;

7. Any network devices to include routers and switches, which are assigned a Media Access Control (MAC) address, a unique number associated with a network adapter and is unique to each computer. A MAC address is burned onto the router during manufacturing and is thus impossible to remove or change. Each MAC address is 12 characters in length, the first six characters contain the ID number of the manufacturer, and the last six numbers represent the serial numbers assigned to the adapter by the manufacturer.
8. All records and information contained on the cellular telephones recovered by OPD in the blue Dodge Durango, as described in Attachment A, that relate to violations of federal law, including violations of 18 U.S.C. § 1029, including:
    a. All texts, contacts, Facebook messages, call history, stored on the cellular phone;
    b. Any information recording ANTHONY HANEL's and COURTNEY CLARK's schedule or travel from the state of Washington on or about January 11, 2019 to the present;
    c. All bank records, checks, credit cards bills, account information, and other financial records.
9. Evidence of user attribution showing who used or owned the cellular phone at the

time of the events described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

10. Address and telephone lists, photographs and videos, travel logs, e-mail messages, internet search histories, history lists, voice messages, internet search queries, text messages, and GPS coordinates, social media messages including, but not limited to Facebook, contained on the cellular phone.

11. Records of Internet Protocol addresses used. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

12. Records and information involving all applications and programs that are downloaded, saved, and/or located on the cellular phone.

13. Records of all deleted records and information, records evidencing attempts to delete records and information, and records and information involving all material on the Devices that were deleted between January 11, 2019 and the present date.

Definitions Applying to Search and Seizure of Computers

14. Records, Documents and Materials

The terms "records," "documents," and "materials" include all of the items described in this Attachment in whatever form and by whatever means they may have been created and/or stored. This includes handmade, photographic, mechanical, electrical, electronic (including e-mail, computer files, Internet histories, bookmarks and all other electronic items that may be found on computer hardware in any form), and/or magnetic forms. It also includes items in the form of computer hardware, computer software, computer documentation, passwords, and/or data security devices.

15. Computer Hardware

Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related

communication devices (such as modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

16. Computer Software

Computer software is digital information which can be interpreted by a Computer and any of its related components to direct the way it works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs).

17. Computer-related Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

18. Computer Passwords and Other Data Security Devices

Computer passwords and other data security devices are designed to restrict

access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "bobby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Blue/Black Samsung Galaxy Note 9 Cell Phone SM N960U, Black LG Cell Phone marked for use with Verizon, Black Samsung Galaxy Cell Phone, Silver Lenovo Yoga Laptop Computer that are all presently in the possession of the United States Secret Service, which is located at 2707 North 108th St., Omaha, NE 68164

Case No. 8:19MJ71

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Nebraska
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before February 26, 2019 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Susan M. Bazis, U.S. Magistrate Judge .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 2-12-19 at 3:57 p.m.

Susan M Bazis
Judge's signature

City and state: Omaha, Nebraska

Susan M. Bazis, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: 8:19MJ71	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

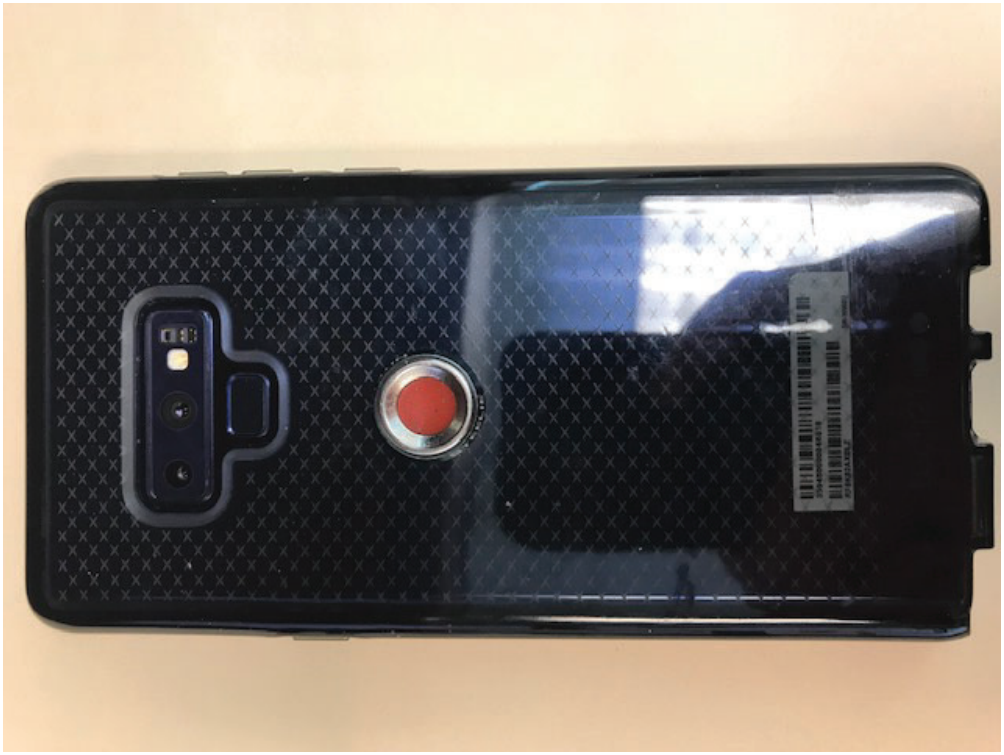
ATTACHMENT A

ITEMS TO BE SEARCHED

This warrant applies to the following items that are all presently in the possession of the United States Secret Service, which is located at 2707 North 108th St., Omaha, NE 68164:

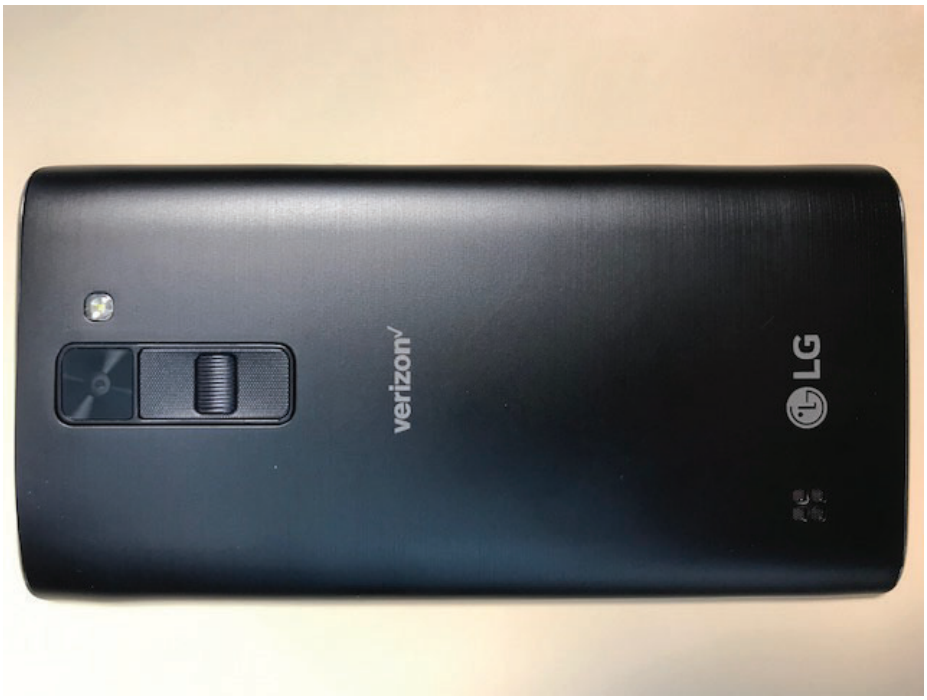
Item #1

Blue/Black Samsung Galaxy Note 9 Cell Phone SM N96OU, IMEI 358621092460188 originally discovered in the suspects' rental vehicle when parked on I-80 East at South 42nd St., Omaha, NE. This item was booked into the computer evidence system of the Omaha Police Department as item #8 under case number AL30847.



Item #2

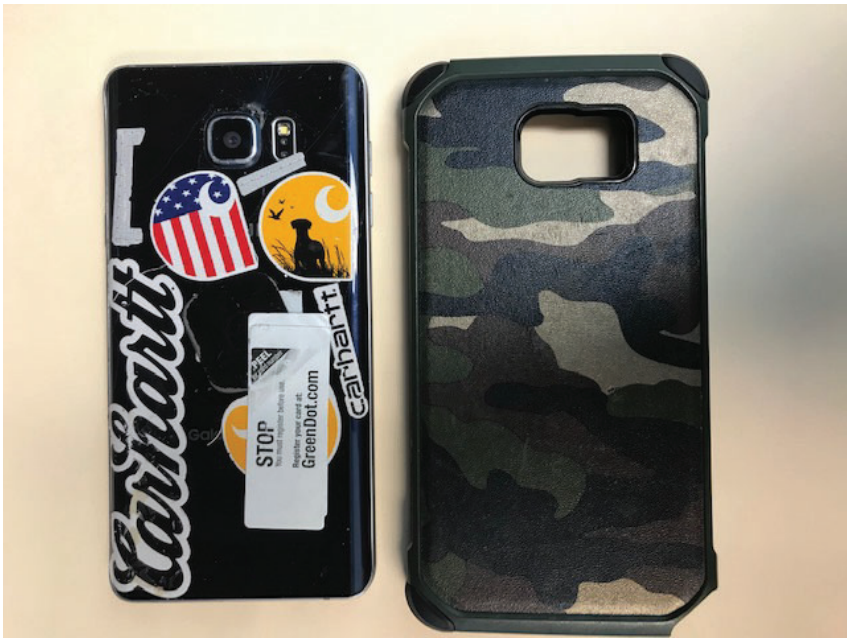
Black LG Cell Phone marked for use with Verizon originally discovered in the suspects' rental vehicle when inventoried at 7809 F St., Omaha, NE 68127. This item was booked into the computer evidence system of the Omaha Police Department as item #15 under case number AL30847.



Item #3

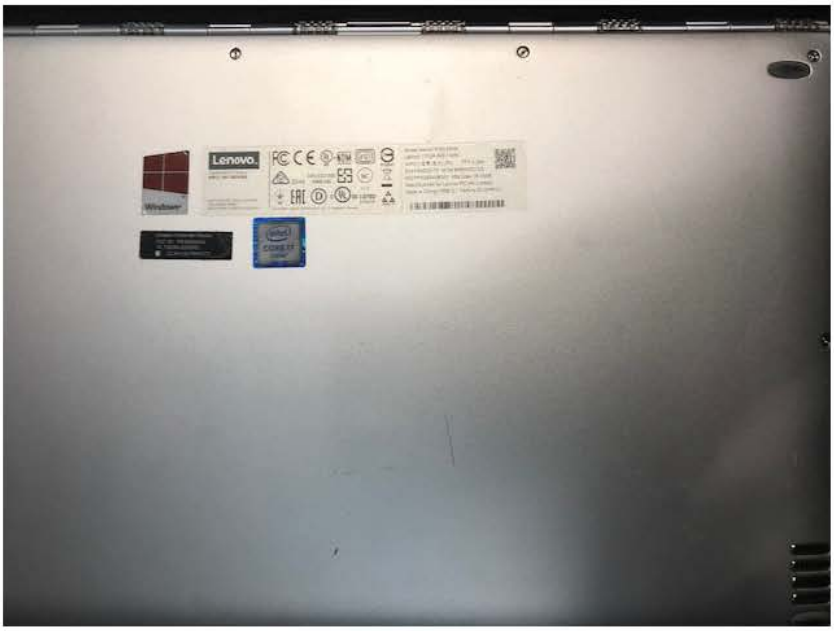
Black Samsung Galaxy Cell Phone IMEI 353756071856926 originally discovered in the suspects' rental vehicle when inventoried at 7809 F St., Omaha, NE 68127. This item was booked into the computer evidence system of the Omaha Police Department as item #16 under

case number AL30847.



Item #4

Silver Lenovo Yoga laptop Computer Serial number PF0D3XYY discovered in the suspects' rental vehicle when inventoried at 7809 F St., Omaha, NE 68127. This item was booked into the computer evidence system of the Omaha Police Department as item #17 under case number AL30847.


Lenovo

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEARCHED

The following items, which may be evidence, fruits, and instrumentalities of violations of Fraud in connection with Fraud and Related Activity in Connection with Access Devices (18 U.S.C. § 1029) are to be searched for and/or seized:

1. Any computers or electronic media, including computer hardware, electronic or magnetic storage devices, such as floppy diskettes, hard disks, backup tapes, CD-ROMs, CD-Rs, CD-RWs, DVD-ROMs, DVD-Rs, DVD+Rs, DVD-RWs, DVD+RWs, optical discs, printer buffers, smart cards, USB thumb drives, USB drives, USB Flash Memory, Firewire Devices, Smart Media, Memory Sticks, Multimedia Cards (MMC), Secure Digital Cards, memory calculators, electronic dialers, Bernoulli drives, electronic notebooks, personal digital assistants, and any data, image or information that is capable of being read or interpreted by computer; that were or may have been used as a means to commit the offenses described in the affidavit.
2. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

3. All records, documents and materials related to ANTHONY JAMES HANEL and COURTNEY LAPARELE CLARK;

4. All records, documents, and materials related to the fraudulent use or creation of access devices;

5. Hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, printouts of computer photographs, graphic interchange formats and/or photographs, and other visual depictions of such graphic interchange formats (including, but not limited to, JPG, GIF, TIF, AVI and MPEG); notations of any passwords that may control access to a computer operating system or individual computer files;

6. Any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation;

7. Any network devices to include routers and switches, which are assigned a Media Access Control (MAC) address, a unique number associated with a network adapter and is unique to each computer. A MAC address is burned onto the router during manufacturing and is thus impossible to remove or change. Each MAC address is 12 characters in length, the first six characters contain the ID number of the manufacturer, and the last six numbers represent the serial numbers assigned to the adapter by the manufacturer.
8. All records and information contained on the cellular telephones recovered by OPD in the blue Dodge Durango, as described in Attachment A, that relate to violations of federal law, including violations of 18 U.S.C. § 1029, including:
    a. All texts, contacts, Facebook messages, call history, stored on the cellular phone;
    b. Any information recording ANTHONY HANEL's and COURTNEY CLARK's schedule or travel from the state of Washington on or about January 11, 2019 to the present;
    c. All bank records, checks, credit cards bills, account information, and other financial records.
9. Evidence of user attribution showing who used or owned the cellular phone at the

time of the events described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

10. Address and telephone lists, photographs and videos, travel logs, e-mail messages, internet search histories, history lists, voice messages, internet search queries, text messages, and GPS coordinates, social media messages including, but not limited to Facebook, contained on the cellular phone.

11. Records of Internet Protocol addresses used. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

12. Records and information involving all applications and programs that are downloaded, saved, and/or located on the cellular phone.

13. Records of all deleted records and information, records evidencing attempts to delete records and information, and records and information involving all material on the Devices that were deleted between January 11, 2019 and the present date.

Definitions Applying to Search and Seizure of Computers

14. Records, Documents and Materials

The terms "records," "documents," and "materials" include all of the items described in this Attachment in whatever form and by whatever means they may have been created and/or stored. This includes handmade, photographic, mechanical, electrical, electronic (including e-mail, computer files, Internet histories, bookmarks and all other electronic items that may be found on computer hardware in any form), and/or magnetic forms. It also includes items in the form of computer hardware, computer software, computer documentation, passwords, and/or data security devices.

15. Computer Hardware

Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related

communication devices (such as modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

16. Computer Software

Computer software is digital information which can be interpreted by a Computer and any of its related components to direct the way it works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs).

17. Computer-related Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

18. Computer Passwords and Other Data Security Devices

Computer passwords and other data security devices are designed to restrict

access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "bobby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.